I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

PETER P. SWIRE* & MARTHA K. LANDESBERG**

Introductory Essay for "2007 Privacy Year in Review"

I. INTRODUCTION

This essay introduces our third issue of Privacy Law Year in Review. With three scholarly articles and thirteen notes by law students, this issue is by far the most comprehensive source for current developments in privacy law, focused on the United States. We hope this issue can be a valuable desktop resource for people who work on the often-bewildering array of information privacy topics.

Some of the most dramatic privacy developments this year were in the area of national security. We have moved into a new phase of thinking about privacy since the events of September 11, 2001. In the immediate aftermath of the attacks, the political system supported the USA PATRIOT Act and other vigorous initiatives for government surveillance. By late 2005, however, major press outlets reported surveillance initiatives that went well beyond what most experts had expected. The elections of 2006 brought a Democratic majority to Congress, along with a new willingness to use congressional hearings to question surveillance programs. As we write this essay in late 2007, Congress is debating an overhaul of the Foreign Intelligence Surveillance Act, and major lawsuits are challenging post-9/11 data collections.

---

* C. William O'Neill Professor of Law and Judicial Administration, Moritz College of Law of The Ohio State University, and Senior Fellow, Center for American Progress. From 1999 until early 2001, Professor Swire served as Chief Counselor for Privacy in the U.S. Office of Management and Budget.

** Director of Policy and Counsel, TRUSTe. Ms. Landesberg was Of Counsel to the law firm of Dorsey and Whitney LLP from 2001–02, and a Senior Attorney in the Federal Trade Commission's Division of Financial Practices from 1995–2001.

In the private sector, this period saw continued ferment on topics including data breach and spyware. Congress has stalled in its efforts to pass a national data breach law. State law innovation, though, has continued, such as new requirements in Minnesota and California to report breaches of medical data. Concerning spyware, the Federal Trade Commission deployed its "unfairness" power to close down a number of companies. Also, the FTC is becoming more active in holding companies responsible for the actions of their marketing affiliates, which has the effect of pushing companies to become more aware of what is done on their behalf by contractors and sub-contractors.

Part II of this essay describes the structure of Privacy Law Year in Review. Part III then summarizes each of the sixteen chapters of the volume.

II. THE TASKS OF PRIVACY LAW YEAR IN REVIEW

The principle goal of Privacy Law Year in Review is to create a trustworthy, non-ideological, and clearly-written annual review of developments in privacy law, with a focus on developments affecting the United States. It is one of three annual issues of *I/S: A Journal of Law and Policy for the Information Society*. Peter Swire ("Peter" in this essay) is Faculty Editor for this issue and co-author of this essay. Peter Shane, also of The Moritz College of Law, is overall Faculty Editor of the journal. Other current *I/S* issues include "Telecommunications" and "Cybersecurity." Information about *I/S* is available at http://www.is-journal.org.

In previous years, privacy expert Sol Bermann was Managing Editor of *I/S* and worked extensively on Privacy Law Year in Review. In 2007, Sol left Moritz to become the first Chief Privacy Officer for the State of Ohio. We congratulate Sol on his new leadership position, although we miss his warmth and his many contributions. Fortunately, Martha Landesberg agreed to work with student note writers this year and to co-author this Introductory Essay. Many readers of this issue will be familiar with Martha from her work on privacy at the Federal Trade Commission and more recently as Director of Policy and Counsel at TRUSTe. Peter and the entire journal staff thank Martha very much for her work; this issue has benefited greatly from her efforts.

As was true for the first two years, we are delighted that this issue of Privacy Law Year in Review will be distributed to all members of the International Association of Privacy Professionals ("IAPP"). Under the leadership of Trevor Hughes, the IAPP has grown rapidly in

recent years and now numbers over 4,500 members. Privacy Law Year in Review is distributed in hard copy to all IAPP members and members also can sign up for passwords to get online access to all *I/S* issues.[1]

We at Moritz continue to work closely with the IAPP to provide high-quality content for privacy professionals, students, and scholars. In the spring of 2007, IAPP published *Information Privacy: Official Reference for the Certified Information Privacy Professional.* Peter, Sol, and students from *I/S* wrote this book, which is now the official study material for the CIPP examination. Peter and others from Moritz have also regularly participated in IAPP events.

Privacy Law Year in Review focuses especially on developments from late 2006 through roughly August 2007. Students began research on their notes in the fall of 2006, working with then-Privacy Issue Editors Kirk Koehler and Gene Park. The editing took place under the leadership of *I/S* Editor-in-Chief Erin Wright and Privacy Issue Editors Megan Engle, Carla Scherr, and Stephen Wolfson. This essay was written in November 2007.

III. ARTICLES BY SCHOLARS IN THIS ISSUE

This issue features three articles by scholars that we think will be of strong interest to IAPP members and privacy experts more broadly.

Professors Joseph Turow and Chris Hoofnagle are the lead authors for "The Federal Trade Commission and Consumer Privacy in the Coming Decade." An earlier version of this research was presented in 2006 at the FTC's Tech-ade Workshop. The version published here updates and confirms the earlier findings with new 2007 polling data.

The key findings pose a challenge to the way privacy policies are used in the United States:

> Large majorities of consumers believe that the term "*privacy policy*" conveys a baseline level of information practices that protect their privacy. In short, "*privacy,*" like "*free*" before it, has taken on normative meaning in the marketplace. When consumers see the term "*privacy policy,*" they believe that their privacy will be protected in specific ways. In particular, when consumers see "*privacy policy*" they

[1] For IAPP members who wish to activate their online access, contact Kimberly MacNeill, IAPP Membership Services Coordinator (207.351.1500 x113/kim@privacyassociation.org).

> assume that a web site will not share their personal information.[2]

The authors thus recommend that the FTC should police the use of the term "privacy policy" in order to "assure that companies using the term deliver a set of protections that meet consumers' expectations."[3] This would be a significant change in the FTC's current practice. For those opposed to such an approach, however, the empirical research poses the following challenge–why should the term "privacy policy" be allowed for practices at odds with what so many consumers understand? There may be good answers to that question, but there have not been any published answers to this question to date.

Professor Rita Marie Cain has written "When Does Preemption Not Really Preempt? The Role of State Law after CAN-SPAM." The CAN-SPAM Act of 2003 created federal rules to govern unsolicited commercial e-mail and generally preempted state anti-spam laws. Professor Cain's article, however, highlights how the specific terms of preemption can have crucial effects. She shows how general state laws prohibiting unfair and deceptive trade practices continue to have effect in the wake of CAN-SPAM. Professor Cain favors a stronger role for state laws to govern spam and makes recommendations for how to accomplish that goal.

The preemption issues in this article are of interest well beyond the topic of anti-spam legislation. Preemption has been a hot-button issue in numerous privacy areas, including financial privacy, medical privacy, and for any proposed federal framework privacy legislation. Professor Cain's article convincingly shows that preemption is not an on/off switch, with either full federal rules or only state rules. Instead, defining "preemption" is a complex process. It is often unclear the extent to which a federal statute is intended to preempt, for instance, claims under state tort, contract, and unfair or deceptive practice laws. From the point of view of consumer protection, preemption should generally not be broader than the scope of the protections created under a federal statute. In legislative debates, however, we are likely to see intense battles in the future over the precise scope of proposed preemption.

In "Tracking RFID," noted cyberlaw expert Jonathan Weinberg examines the trajectory and diffusion of Radio Frequency

---

[2] Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 ISLJP 723 (2007-08).

[3] *Id.* at 724.

Identification ("RFID") technology. By delving deeply into the technology and history of RFID tags, Professor Weinberg shows how the lack of a business case has initially slowed diffusion of RFID tags for many applications. Because the cost of tags will come down over time, however, he believes we must prepare for a world that has pervasive RFID, along with networked devices that will routinely collect and process the resulting information.

Professor Weinberg sees important societal benefits from the use of RFID as inventory control tags. He cautions, though, that it is easy to exaggerate the value of maintaining the ability to keep such tags live after the point of sale. He would favor a rule generally requiring that inventory-control RFID tags attached to individual retail items be clearly labeled and easily removable.

Professor Weinberg is distinctly more skeptical of the benefits of RFID tags on government identification credentials. He concludes that serious privacy threats make it almost always undesirable for government identity credentials to incorporate RFID. He concludes: "[W]hile the inclusion of digitized and encrypted information on identification documents does provide important anti-forgery and anti-tampering benefits, that information need not be transmitted *wirelessly*."[4]

IV. AN OVERVIEW OF PRIVACY LAW IN 2007

The notes in this year's Privacy Year in Review are grouped into the following five categories: national security surveillance and national authentication systems; government surveillance in context, for e-mails, location, and video; privacy on the Internet and in organizational databases; sensitive financial and medical information; and international issues.

A. NATIONAL SECURITY SURVEILLANCE AND NATIONAL AUTHENTICATION SYSTEMS

The past two years have seen the biggest battles about national security surveillance since the Watergate era.[5] Notes by Austin

---

[4] Jonathan Weinberg, *Tracking RFID*, 3 ISJLP 824 (2007–08).

[5] For some of Peter's writing on national security surveillance, *see Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 260 (2006); *Legal FAQs on NSA Wiretaps*, CENTER FOR AMERICAN PROGRESS, Jan. 30, 2006, http://www.americanprogress.org/issues/2006/01/b1389573.html; *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004).

Anderson and Stephen Wolfson describe the three overlapping sets of disclosures that led to legal drama in 2006 and 2007. First, The New York Times published details of what came to be called the Terrorist Surveillance Program. This program apparently authorized wiretaps outside of the Foreign Intelligence Surveillance Act ("FISA") when one of the parties was outside of the United States and there was a reasonable basis to believe that at least one of the parties had links to a terrorist organization. The program was declared unconstitutional by a district court in 2006, but the court of appeals reversed on the basis that no plaintiff had standing to sue. In early 2007, Attorney General Gonzalez wrote a letter to the Senate Judiciary Committee saying that the administration would continue the surveillance program under the supervision of the Foreign Intelligence Surveillance Court. In August, the Congress passed the Protect America Act to modify and update some provisions of FISA. That Act sunsets, however, in early 2008.

The second national security surveillance controversy arose from a USA Today report that the government had received call detail records from phone companies for tens of millions of Americans. Under the Stored Communications Act, each individual whose call detail records are improperly disclosed is entitled to statutory damages of at least $1,000. Class-action lawsuits have thus been filed, seeking damages in the tens of billions of dollars–if the records of 40 million Americans were illegally disclosed, then damages would be $40 billion. The third controversy derived from testimony by former AT&T employee Mark Klein, who stated that a special room was built to contain equipment that allowed the National Security Agency to get a direct feed from major entry points of voice and data traffic into the United States. The Electronic Frontier Foundation filed a lawsuit based on information from Klein and other sources.

The administration and telecommunications companies have had two major responses to the lawsuits. First, they have defended themselves with the "state secrets privilege," arguing that courts should not allow inquiry into the details of the national security surveillance. Second, they have sought legislative change to FISA and related statutes to allow such actions. The Protect America Act, for instance, appeared to give significant authorization to the sorts of surveillance conducted under the Terrorist Surveillance Program. For future conduct, it also created civil immunity for telecommunications providers who cooperated in good faith with government requests. Intensive legislative debates and litigation on national security surveillance will likely continue for the foreseeable future.

Debra Milberg's note examines the authentication controversies surrounding the REAL ID Act of 2005 and proposals to require stricter authentication for voting. The note describes the rationale for

minimum national standards for driver licenses under the REAL ID Act. It also explains privacy, security, cost, federalism, and other critiques. At least seventeen states have now passed laws or resolutions opposing REAL ID or rejecting its implementation.[6] The political and substantive objections to REAL ID create a major obstacle for those policymakers who believe that stricter authentication should be part of overall American policy to fight terrorism.[7]

The same note canvasses the current legal battles about authentication for voters. The Help America Vote Act of 2002, among its other provisions, requires states to maintain a statewide official voter list that can be verified against the state motor vehicles database. As states wrestle with this mandate, there have been privacy and security objections to how the databases are maintained. Meanwhile, seven states now require a photo ID to vote and an additional eighteen states require either a photo or some additional level of authentication. Voting authentication has become a partisan political issue in many states, with Republicans saying that stricter rules will reduce fraud and Democrats denying the link to fraud and saying that stricter rules are designed to disenfranchise Democratic-leaning voters. Many of these state laws have been subject to challenge in court. The note analyzes the complex current landscape of voting authentication and also highlights the sorts of debates that are likely to occur more generally for new authentication systems.

B. GOVERNMENT SURVEILLANCE IN CONTEXT, FOR E-MAILS, LOCATION, AND VIDEO

Three notes provide updates for how government surveillance is governed in specific contexts: for location information, such as by cell phone location or global positioning technology; for video surveillance; and for electronic communications, such as e-mails.

For these categories of surveillance, two lines of doctrine have significantly limited the application of Fourth Amendment rules requiring warrants for government searches. First, Supreme Court cases dating to the 1970's have announced the "third party" doctrine. When individuals store records with third parties, such as banks or

---

[6] Anne Broache, *Is REAL ID Plan on its Deathbed?*, CNET NEWS.COM, Nov. 2, 2007, http://www.news.com/8301-10784_3-9809992-7.html.

[7] One of the co-authors, Peter, is engaged in a project at the Center for American Progress concerning how authentication should be understood for diverse issue areas, including national and homeland security, immigration, voting, computer security, and privacy and civil liberties.

telephone companies, those third parties are constitutionally permitted to turn the records over to the government without a warrant. Laws such as the Right to Financial Privacy Act or the Electronic Communications Privacy Act may create statutory limits on government access, but the Fourth Amendment itself has been held not to apply. Second, the Fourth Amendment does not generally set limits on the ability of government agents to gather information that is in plain view, such as the fact that an individual is driving down the street in a car.

Both of these doctrines are relevant to Kevin Keener's note on surveillance of location information. American autos are increasingly equipped with navigation tools that use global positioning systems ("GPS"). To date, information held by the operators of the GPS appears to be covered by the third party doctrine, and information about the location of the car (except perhaps when it is parked within the garage of a house) comes under the plain view doctrine. As for cell phones as tracking devices, the third party doctrine again may well apply for government access to location information, although there has begun to be disagreement in the courts about this issue.

For Carla Scherr's note on video surveillance, the plain view doctrine generally allows the police to see (in person or by video) what is happening in public or in plain view. Ms. Scherr explains the law governing the rapidly increasing use of video surveillance. She proposes factors to use in privacy policies or statutes to address the privacy problems that arise from pervasive video surveillance. The factors she identifies would include the distance between the camera and the subject and the degree of magnification, whether specific individuals are selected and tracked, whether individual subjects are identified, the durability and distribution of the images, the likelihood of unauthorized image use and modification, and whether images are correlated with data from other sources.

Erin Wright's note examines recent developments in the privacy of electronic communications, especially e-mail. In 2007, the United States Court of Appeals for the Sixth Circuit appeared to announce a major exception to the Fourth Amendment's third-party doctrine. In *Warshak v. United States*, the Court held that the plaintiff maintained a reasonable expectation of privacy in his stored e-mails because the Internet Service Provider did not access the e-mails in the ordinary course of its business.[8] In essence, the Court held that the content of e-mails deserve the same constitutional protection as phone calls. Ms.

[8] 490 F.3d 455 (6th Cir. 2007).

Wright explains how the *Warshak* opinion built on substantial writing by law professors including Patricia Bellia, Susan Freiwald, Deirdre Mulligan, and Peter Swire, who all signed amicus briefs in the case on the side of plaintiff. On the other hand, the Sixth Circuit has recently granted en banc review, and Professor Orin Kerr has written in detail on why he believes the panel decision should be overturned.[9]

C. PRIVACY ON THE INTERNET AND IN ORGANIZATIONAL DATABASES

Each year, the Privacy Year in Review highlights recent privacy developments concerning the Internet, new technologies, and organizational databases. Notes this year focus on data breaches, spyware enforcement, phishing, and RFID tags.

Responding to data breaches has continued to be a major issue for both public- and private-sector organizations. Michael Jones's note updates the many recent developments concerning data breach. It chronicles the high-profile breaches, including the loss of millions of veterans' Social Security numbers from a Veterans' Administration laptop. One important result of that breach was new guidance from the Office of Management and Budget to all federal agencies to create stricter procedures for responding to breaches. Another federal initiative was the report of the President's Identity Theft Task Force in April 2007.

For private-sector organizations, the Federal Trade Commission has continued to bring cases against companies whose security practices it found to be unfair or deceptive. Private-sector organizations have been deeply engaged in discussions of proposed federal legislation for data breach but substantive disagreements and jurisdictional battles in Congress have blocked action thus far. Mr. Jones examines key issues in state data breach law, such as the trigger for notice to data subjects and the role of encryption. The states have continued to legislate heavily in this area, with states such as Minnesota and California breaking new ground with notice required for loss of medical records. In short, a large and growing array of organizations are facing compliance responsibilities in connection with any breach of their databases.

Another focus of federal attention has been spyware. Megan Engle's note examines recent spyware enforcement actions by the Federal Trade Commission. The Commission obtained stipulated

---

[9] Professor Kerr's writings on the topic are gathered at The Volokh Conspiracy, http://volokh.com/posts/1182208168.shtml (last visited Jan. 20, 2008).

permanent injunctions in the *Odysseus Marketing, Inc., ERG Ventures, LLC.* and *Enternet Media, Inc.* cases that effectively shut down the defendants' spyware distribution operations. Instead of relying solely on its "deception" authority, it is noteworthy that the Commission also brought these cases under its "unfairness" authority. The alleged unfairness was the bundling of purportedly "free" or otherwise innocuous software with spyware that allegedly acted surreptitiously in a variety of ways, including altering browser and home page settings, inserting advertising toolbars into browsers, disabling anti-virus and anti-spyware software, and otherwise degrading the computers' performance. The Commission found that these harms, along with the time and money spent by consumers in trying to fix the problems and uninstall the software, could not have been reasonably avoided by consumers and were thus "unfair" under Section 5 of the Federal Trade Commission Act.

The Commission also directed its attention to the extensive affiliate networks by which purveyors of spyware and adware companies often distribute their software. In the *Enternet Media Inc.* case, the Commission obtained a separate permanent injunction against one such affiliate. That site was a distribution point for advertisements for free browser and security upgrade software that was in fact "malware" designed to disrupt computer functionality. Affiliates' practices were also at the center of the Commission's settlements with adware companies DirectRevenue, LLC, and Zango, Inc. These cases included unfairness claims based upon the surreptitious installation of adware on consumers' computers by the respondents' affiliates. The cases are important because they define the components of an acceptable model for the distribution of adware, including notice and prior consent, an easy-to-use uninstall, a consumer complaint mechanism, and the labeling of advertisements so consumers know the source of the ads and how they can control them. Just as importantly, the settlements require DirectRevenue[10] and Zango to bind their affiliates (and, in turn, their affiliates' subcontractors) to the settlement terms. There is every reason to believe that the Commission will continue its intensive focus on the adware market, and to hold adware companies responsible for their affiliates' and distributors' practices.

Another form of Internet fraud is "phishing," where a fraudster, in the classic case, sends an e-mail to a consumer claiming to be a respected organization (bank, employer, etc.) that needs to "verify"

[10] Since the settlement agreement, DirectRevenue, LLC has gone out of business. *See* DirectRevenue, http://www.direct-revenue.com (last visited Jan. 20, 2008).

personal information. If the consumer replies, the fraudster uses the information for identity fraud, such as gaining access to the consumer's bank account. Rasha AlMahroos' note updates developments in phishing, including descriptions of variants such as "spear phishing," "pharming," and "vishing." The note discusses the work of the Anti-Phishing Working Group and other efforts to combat the problem, as well as technological counter-measures, including SenderId and DKIM.

As Ms. AlMahroos writes, several states have now adopted anti-phishing laws. At the federal level, statutes such as the CAN-SPAM and SAFE WEB Acts may address some phishing problems, and there have begun to be anti-phishing proposals in Congress. The FTC this year also held a Spam Summit, another in a series of public workshops focusing on fraudulent e-mail and authentication.

Laura Ulatowski's note on Radio Frequency Identification ("RFID") complements Jonathan Weinberg's article on the same topic. The note provides a primer on RFID technology. It highlights current uses of RFID tags by government, such as in identification documents, and by private industry, including the fight against counterfeit prescription drugs. The note summarizes the arguments for and against the widespread adoption of this technology for tracking human activity and the role of future legislation. It also highlights the privacy issues posed by potential uses of RFID and discusses current private-sector efforts to identify best practices for use of RFID tags.

D. SENSITIVE FINANCIAL AND MEDICAL INFORMATION

Each year Privacy Year in Review updates developments in the regulated areas of financial and medical privacy. For 2006 and into 2007, the changes in these areas were incremental and thus likely of greatest interest to persons in the financial and medical fields.

Sarah Exten's note updates issues of financial privacy. The biggest privacy controversy this year surrounded the U.S. Government's access, as part of its anti-terrorist operations, to information in the SWIFT database of international financial transactions. Belgium declared the transfer of data illegal under its national data protection law, and there have been strong expressions of concern by other EU privacy regulators.

In other developments in financial privacy, the Financial Regulatory Relief Act of 2006 clarified that certified public accountants are exempt from the Gramm-Leach-Bliley disclosure provisions. In a recent case about the use of financial services information in litigation, the Mississippi Supreme Court held that

customer lists otherwise protected by the Act may be discoverable in civil litigation under certain circumstances. For the Fair Credit Reporting Act, the United States Supreme Court held in *Safeco Insurance Co. of America v. Burr* that disadvantageous initial rates offered to applicants for new insurance policies may be "adverse actions" and thus subject to the Act's adverse action notice requirement. The Supreme Court also clarified the scope of "willful" violations of the Act to include actions taken with reckless disregard for the Act's requirements. Such "willful" actions subject the violator to civil liability including actual, statutory, and punitive damages.

Cicely Tingle's note discusses developments in medical privacy. Under the Health Insurance Portability and Accountability Act, a source of continuing controversy has been the low levels of criminal and civil enforcement. Ms. Tingle describes the criminal cases brought to date by U.S. Attorney offices (none have been brought by Main Justice). She also reports that 30,000 complaints had been filed with the Office of Civil Rights by the end of August 2007, but no civil money judgments or other financial penalties have yet been assessed. On health information technology, Ms. Tingle provides updates on four major contracts that HHS has pursued in the area. She updates recent proposals for health IT legislation, and briefly discusses the debate concerning health IT and preemption of state privacy laws.

E. INTERNATIONAL ISSUES

Although previous issues of Privacy Year in Review have examined key privacy issues in the European Union and elsewhere in the world, Carla Bulford's note is the first to examine in detail the Asia Pacific Economic Cooperation ("APEC") Privacy Framework. It is a truism that technology enables vast amounts of data to cross international boundaries, presenting chronic problems for national privacy regimes. How nations address information privacy is a matter of culture and history and negotiating the differences among privacy regimes can be a significant challenge for government agencies, individuals, and businesses.

Ms. Bulford's note looks closely at the APEC Privacy Framework's nine privacy principles, which are intended to be adapted for implementation, in both regulatory and self-regulatory contexts, across APEC economies. The article contrasts the Framework's approach to information privacy with legislative models in the United States and Europe, and speculates on the effects the Framework could have on international data flows beyond APEC. It also discusses current efforts under the auspices of APEC's Electronic Commerce

Steering Group to conduct a Pathfinder, or pilot project, testing a system of regulatory and self-regulatory privacy rules that would implement the Framework for cross-border transfers of personal data within APEC.

V. CONCLUSION

All of us who work on information privacy law must continually respond to new technologies. Our privacy volume this year, for instance, examines the effects of new technologies such as RFIDs, location tracking by GPS and cell phones, and video surveillance. New technologies lead to new information systems and push the courts and regulators to decide the terms for government and private access to the new streams of data.

Another source for change comes from the political system. We write this essay as voters prepare for the first primaries of the 2008 election. The attacks of 9/11 will be more than seven years in the past by the time of that election and the tradeoffs of privacy and security could well be different then they were when the USA PATRIOT Act was passed in 2001. The next president, whether Republican or Democrat, could very well make choices about privacy that differ significantly from those made by the Bush Administration.

The politics of privacy are complex and surely do not follow simple partisan lines. Many Republicans, for instance, have long been skeptical of government intervention and thus have historically supported protections against such intrusions. For some, private-sector activities pose much less risk to privacy. Democrats, to generalize a bit, are more inclined than their Republican counterparts to support restrictions on private-sector activities that they believe negatively affect privacy; but they, too, are wary of government intrusions. Yet, there is no doubt that the coming election will draw clear distinctions along party lines. There is a distinct possibility that a Democrat will be elected to the presidency in 2008 who may place more emphasis on privacy policy for the private sector as well as for government. To take just one example, Senator Hillary Clinton has pledged to appoint a White House official to coordinate privacy policy, a step that President Bush chose not to take.[11]

---

[11] Sen. Hillary Rodham Clinton, Remarks of Senator Hillary Rodham Clinton on Privacy to the American Constitution Society (June 16, 2006) ("create a high-level privacy czar in the Office of Management and Budget"), *available at* http://www.senate.gov/~clinton/news/statements/details.cfm?id=257288.

Privacy professionals in 2008, therefore, must prepare, not only for new developments in the broad array of specific issues surveyed by this volume of our journal, but also for the possibility that there will be significant changes in privacy law and policy generally in the coming years.